REMARKS

Claims 15-29, 35, 37, 38, 41 and 42 are pending in this application. Claims 15 and 35 have been amended.

Claims 15-29 and 35, 37, 38, 41 and 42 were rejected under 35 USC §103(a) as being unpatentable over Carter (U.S. Patent No. 5,787,175) in view of Follendore, III (U.S. Patent No. 6,011,847) and further in view of Tada et al. (U.S. Patent No. 6,178,422). The Examiner stated that the combination of Carter, as modified by Follendore, III does not teach "a plurality of annotations generated by an annotation author, wherein access to the plurality of annotations is available to the users designated by the annotation author as having access to the plurality of annotations" and "a second multi-key encryption table comprising at least one multi-key encryption component associated with each authorized annotation user." The Examiner cited Tada et al. for teaching these features, citing col. 5, lines 37-65 and col. 6, lines 20-24 and Figs. 2, 3 and 8 of Tada et al. Applicant respectfully disagrees.

Applicant's secure content object provides a means of distributing and controlling access to a document and any annotations associated with the document. The secure content object may be used in those instances when multiple authors may wish to make annotations or comments to a common electronic document and control access (and knowledge of) their annotations among other users. For example, the original electronic document may have no restrictions on viewing (all users may view it), so it is not encrypted. One or more users/authors (including the original author) may wish to make annotations or comments to the electronic document. Each annotation author may wish to limit access to one or more of the annotations. Each such annotation may be encrypted and access limited to certain users. When an authorized user inputs its user authorization information, only those portions of the document and any authorized annotations are displayed. The user sees, in the clear, only those portions of the document to which it has access.

Carter teaches a collaborative encryption method that uses structures in the prefix portion to restrict access to the information stored in the data portion. Users who are currently members of the collaborative group can readily access the information (see abstract). Follendore III teaches a cryptographic control system for managing the encrypting keys, a key management system which keeps track of keys used with a particular message, but also maintains the justification for the use of that key and the justification for the different categories of personnel access and the criteria used for selecting the communication system (see col. 2, lines 20-26). Tada et al. teaches an information registration method and document information system. Tada et al. teaches a system which registers each document in the system and assigns an access code to each document. In Tada et al.'s document management system, users allowed to access a document are registered as attribute information for each group to which the users belong.

1. Tada et al.'s document system does not use encryption. All documents are stored in the database and no document is permitted to be retrieved by a user unless the user's attribute information is registered with that document. In contrast, in Applicant's secure content object, anyone can possess the secure content object, since the important aspects of the information contained within it are encrypted. While anyone can possess a secure content object, only authorized users can decrypted portions of the document or annotations stored in the secure content object.

2. Tada does not teach "a plurality of annotations generated by an annotation author, the plurality of annotations having been encrypted with an annotation encryption key, wherein access to the plurality of annotations is available to the authorized annotation users comprising the annotation author and those users in the first set having been designated by the annotation author as having access to the plurality of annotations (col. 5, lines 37-65 and col. 6, lines 20-24).

Tada et al. as noted above, does not teach encryption; documents are provided to authorized users in the clear if the user's attribute information is attached to the document desired to be retrieved.

Tada et al. teaches only complete documents stored in the document management system. Tada et al. does not differentiate between the document and any annotations that may be associated with it. As best Tada et al. is understood, any annotations (edits, for example, see col. 9, lines 1-5) would be treated as part of the original document and any authorized user would have access to the annotations as well as the original document.

3. The combination of Carter and Follendore III and Tada et al. does not teach Applicant's secure content object. None of the references cited teaches encrypting annotations

associated with a document differently than encrypting the original document (Tada et al. does not teach encryption of the documents stored in its system). None of Carter, Follendore III or Tada et al. teaches treating access to annotations associated with a document differently than treating the document itself. Therefore, any authorized user of a particular document in Carter, Follendore III or Tada et al. would have the same access rights to any annotations associated with the document.

Even if one skilled in the art were motivated to combine Tada et al. with Carter (or Carter and Follendore III), he would not arrive at Applicant's secure content object. Combining Tada et al. with the collaborative document control of Carter (or Carter and Follendore III) would only result in registering the encrypted documents of Carter in the Tada et al. system and assigning a Tada et al. access code (which is in the clear) to each document. Users would be able to retrieve encrypted documents stored in the Tada et al. document management system based on the attribute information registered to each document. Users would still have to submit their authorization code to decrypt the retrieved document.

Independent Claims 15 and 35 are believed to be allowable. Since Claims 16-29 depend from Claim 15 and Claims 37, 38, 41 and 42 depend from Claim 35, they are also believed to be allowable. Claims 15-29 and 35, 37, 38, 41 and 42 are believed to be in condition for allowance.

No additional fee is believed to be required for this amendment; however, the undersigned Xerox Corporation attorney hereby authorizes the charging of any necessary fees, other than the issue fee, to Xerox Corporation Deposit Account No. 24-0025.

Reconsideration of this application and allowance thereof are earnestly solicited. In the event the Examiner considers a personal contact advantageous to the disposition of this case, the Examiner is requested to call the undersigned Attorney for Applicant, Jeannette Walder.

Respectfully submitted,

Jeannette M Walder

Jeannette M. Walder
Attorney for Applicant
Registration No. 30,698
Telephone: 714 565-1700

Xerox Corporation
Santa Ana, California
Date: November 2, 2005